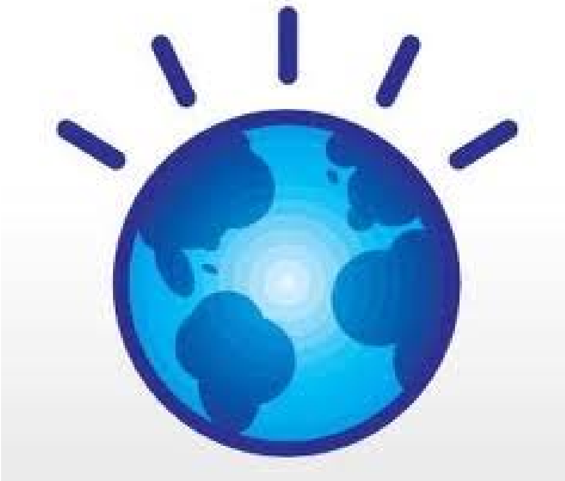
Cyber Physical Systems: Computing for The Smart New World

Sang Hyuk Son

CPS Global Center
DGIST

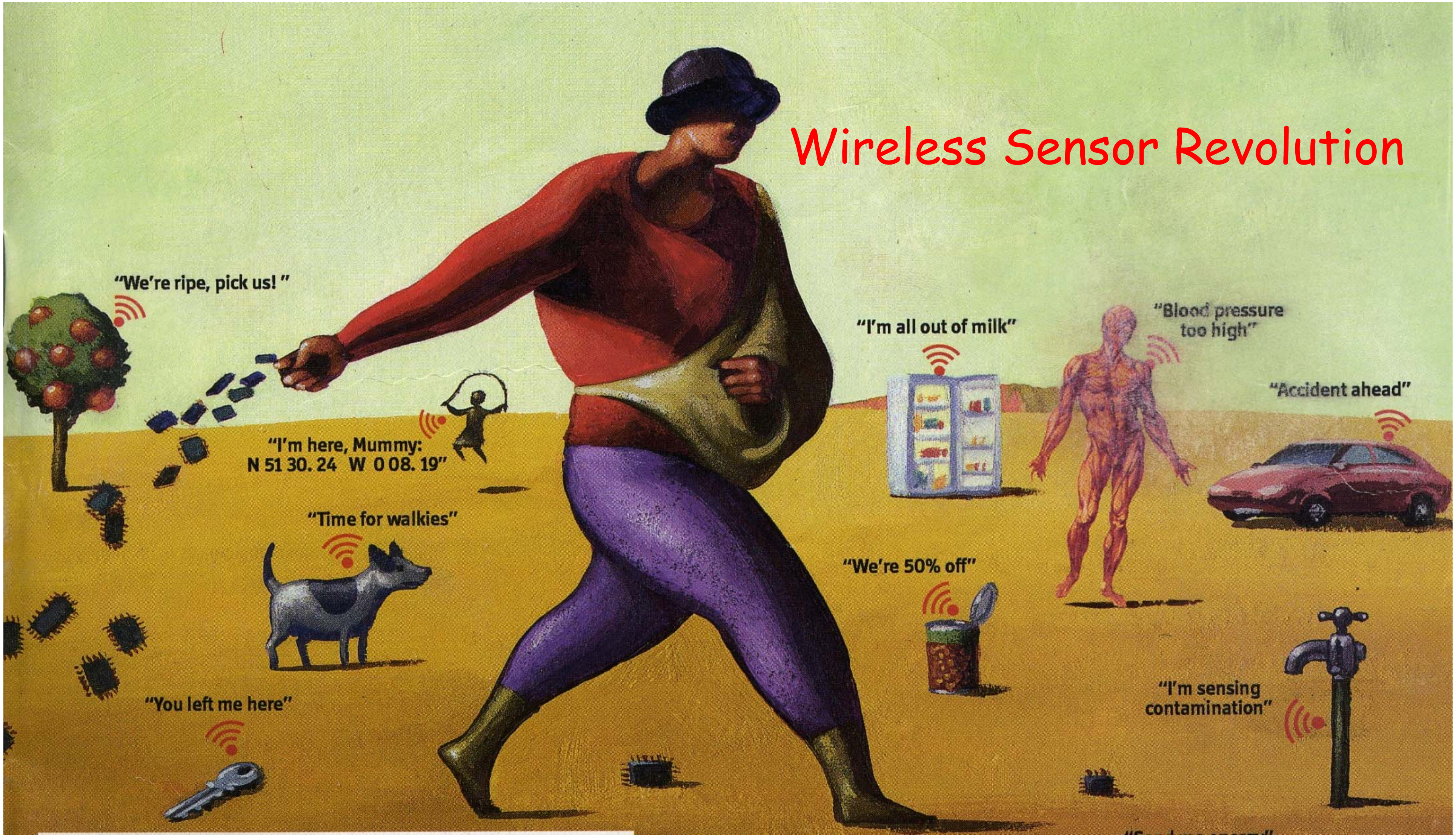
2013.1.31

When Everything is Smart



Smarter Planet by IBM

When Everything Talks

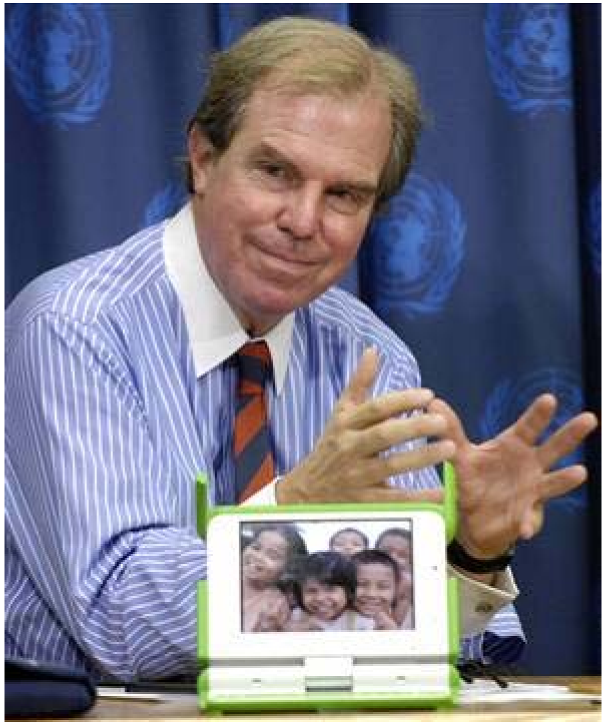


Source: The Economist

Key to the Smart World: Computing

- Ubiquitous
- Practical
- Profound
- Multi-disciplinary
- Enabling scientific and technological advances
- Transforming daily life
- Major contributor to prosperity and well-being of society

Computing is …



Computing is not about computers any more. It is about living.

Nicholas Negroponte

MIT Media Lab

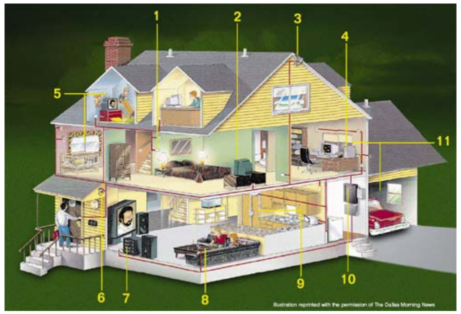
One Laptop per Child Association

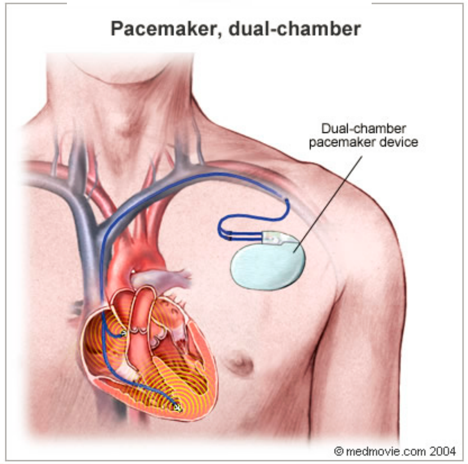
Trends

- Device proliferation
  - Embedded everywhere
  - Generate tons of data

    35 ZB by 2020

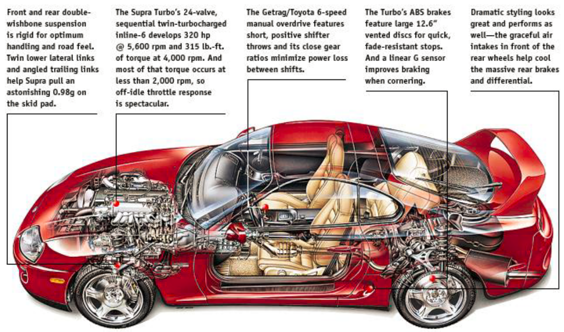
    (zettabyte = 1 trillion GB)

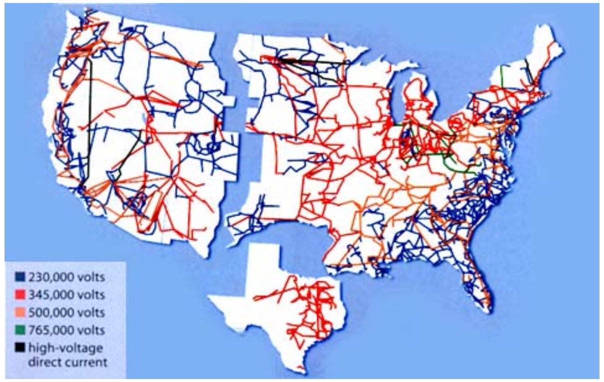


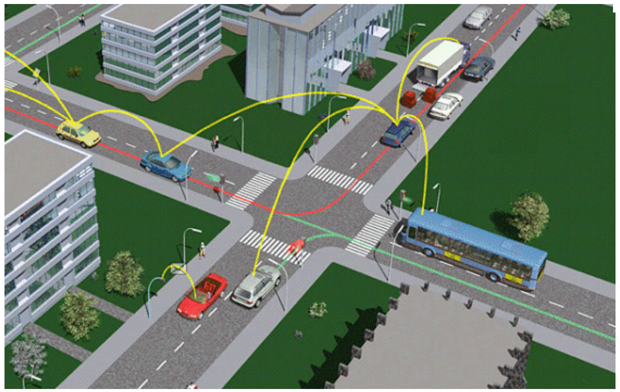


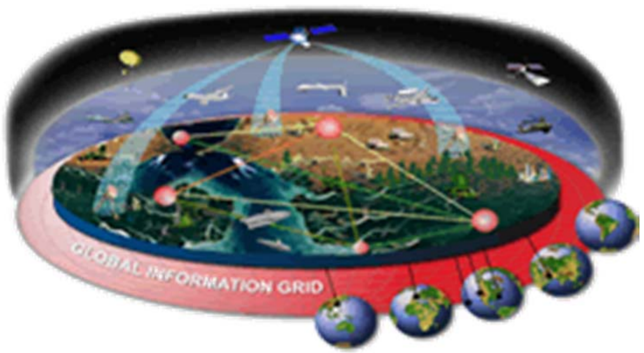
Trends

- Interconnected and integrated
  - At multiple levels and scales
  - No man is an island (John Donne)



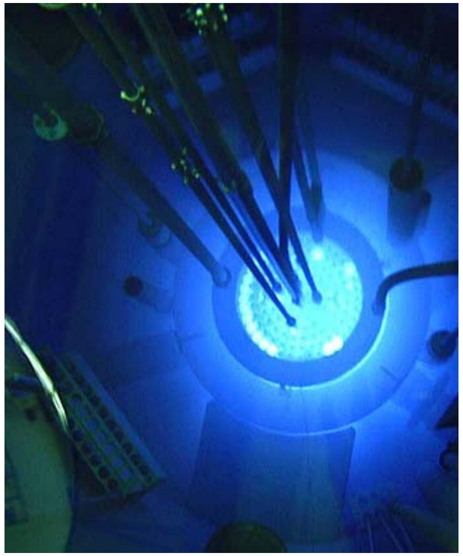


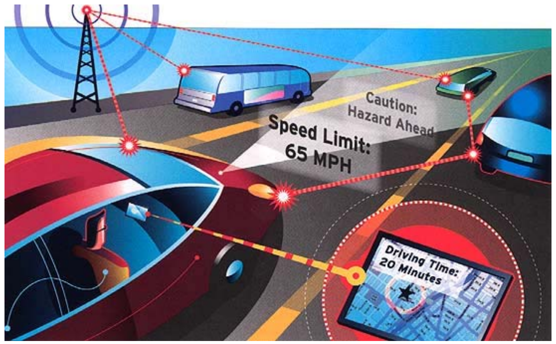




Trends

- Autonomy and control
  - Human-in-the-loop not fast enough
  - Closing the loop with increased autonomy and control

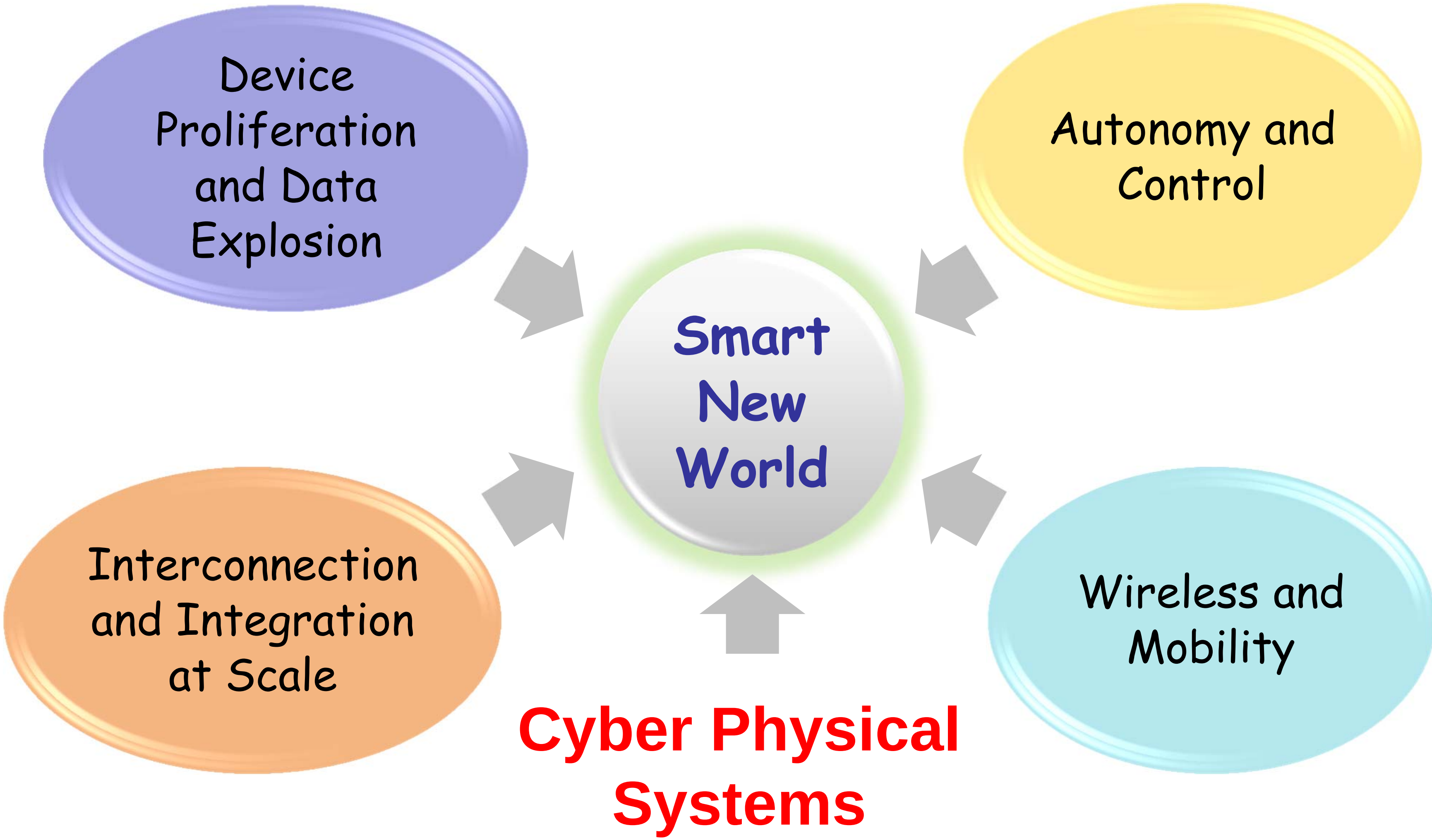




Age of The Smart New World

- Trends
  - Proliferation of devices: embedded everywhere
  - Interconnection and integration at multiple dimensions
  - Autonomy and control
  - Wireless and mobility
  - Embedded devices + wireless networks + mobile computing => Transforming the physical world into a highly connected smart environment, which is huge, diverse, complex, and highly dynamic
  - Internet of Things (IoT): The physical world is being connected to the Internet – everything talks

Confluence of Trends



What are Cyber Physical Systems?

- Cyber

  - Computation, communication, and control that are discrete, logical, and algorithm-based

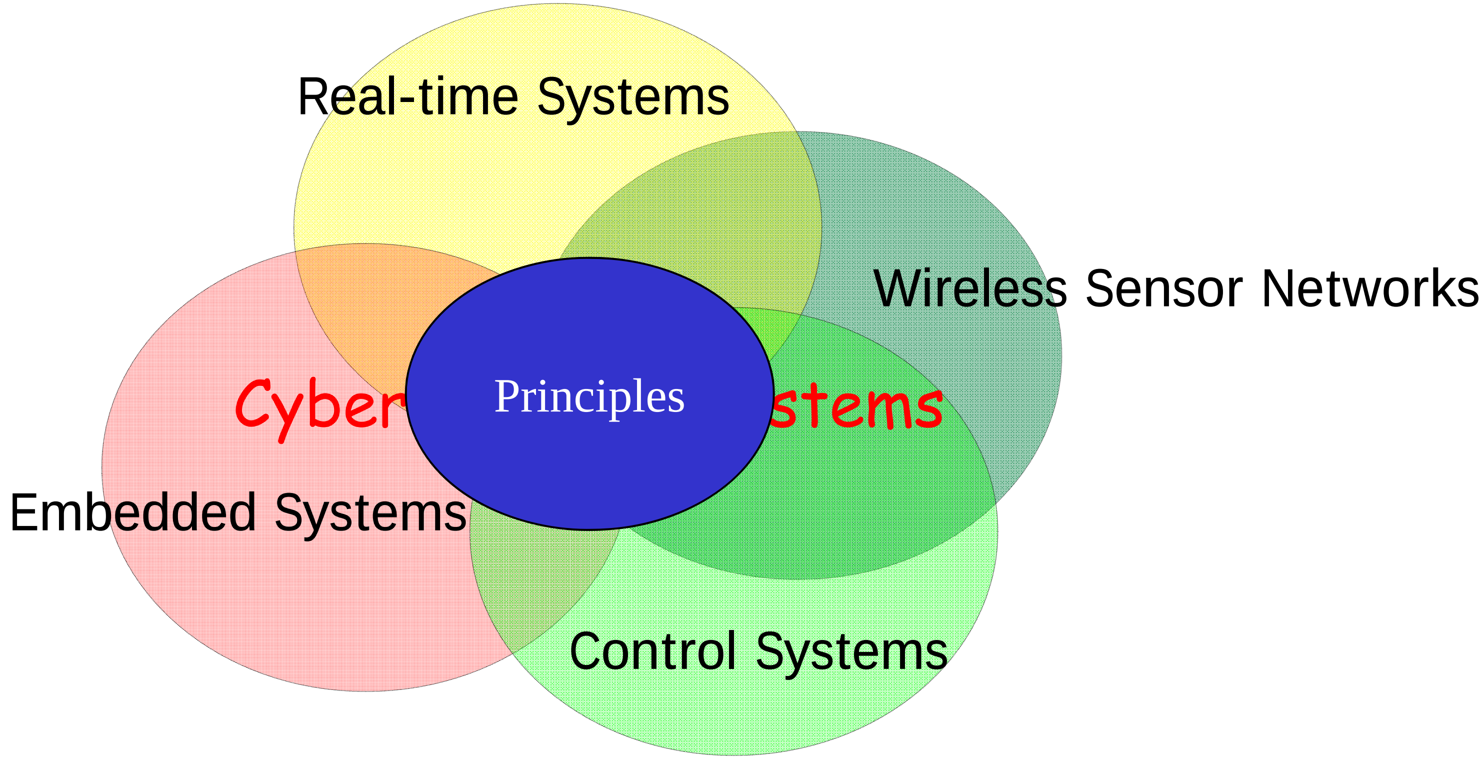
- Physical

  – Natural and human-made systems governed by the laws of physics and operating in continuous time

- Cyber Physical Systems

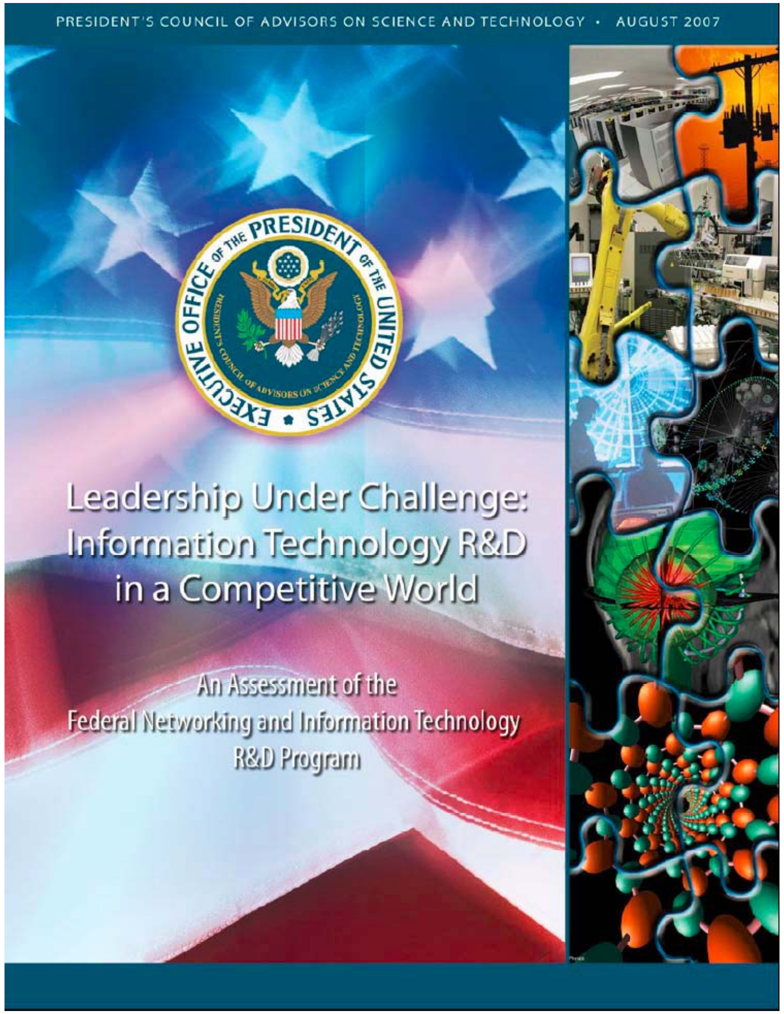
  – Systems in which the cyber and physical components are tightly integrated at all levels and scales

Constituents of CPS



Important?

- In USA, 2007 PCAST report
  - CPS given highest priority
  - Essential to security and competitiveness
  - Our lives depend on them
- 2010 PCAST report
  - Calls for continued investment in CPS research
- EU: ARTEMIS & FP7



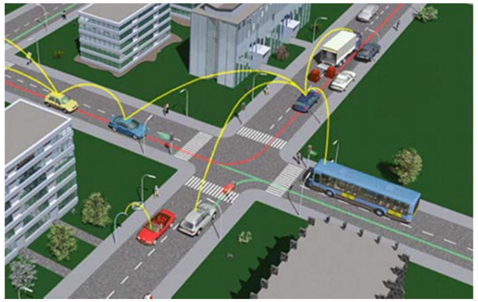
* PCAST: President's Council of Advisors on Science & Technology

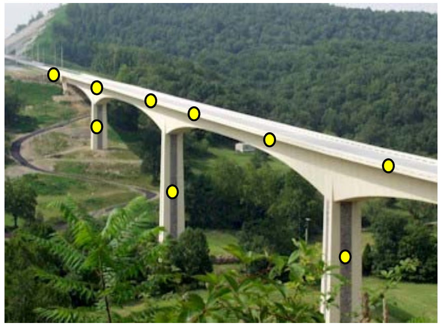
Applications of CPS

Environment monitoring

Weapon systems

Intelligent transportation

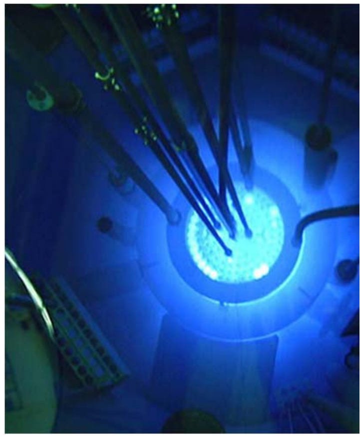




Infrastructure

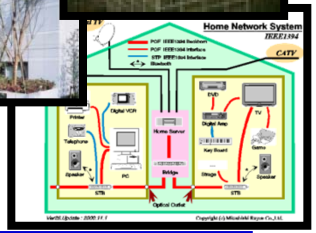
Medical & healthcare

Energy



Smart grids

Smart buildings



Example Opportunities

- Transportation
  - Improved use of highways and airspace
  - Safer, smarter, and energy-efficient cars & planes
- Energy and smart buildings
  - Net-zero energy buildings and smart homes
  - Distributed microgrids
- Healthcare and medical services
  - Effective and preventive in-home care
  - Interoperating medical devices to reduce accidents
- Infrastructure health monitoring

Challenges Arise

- Co-existence of Booleans and Reals
  - Discrete systems in a continuous world

- Uncertainty
  - Scale: world covered by trillions of sensors
  - Complexity: systems of systems
  - Interactions of physical properties, wireless communication, and control
  - Human (in the loop) participation

- Reasoning about uncertain complex systems

Software is The Key

It's the software that determines system complexity.

- Good: You can do anything in software!
- Bad: You can do anything in software!
- Ugly: It's hard to get it right!

Anything is possible but how can we do it right?

Answer: More funding!

Openness and Robustness

- CPS should support operating in open and dynamic environments, with possible errors and failures
- Openness
  - Correct execution of systems when operating environment can change
  - Tasks and available resources may change
- Robustness
  - Need to consider possible dynamics
  - Need to consider uncertainties, errors, and failures
  - Real-time support is required

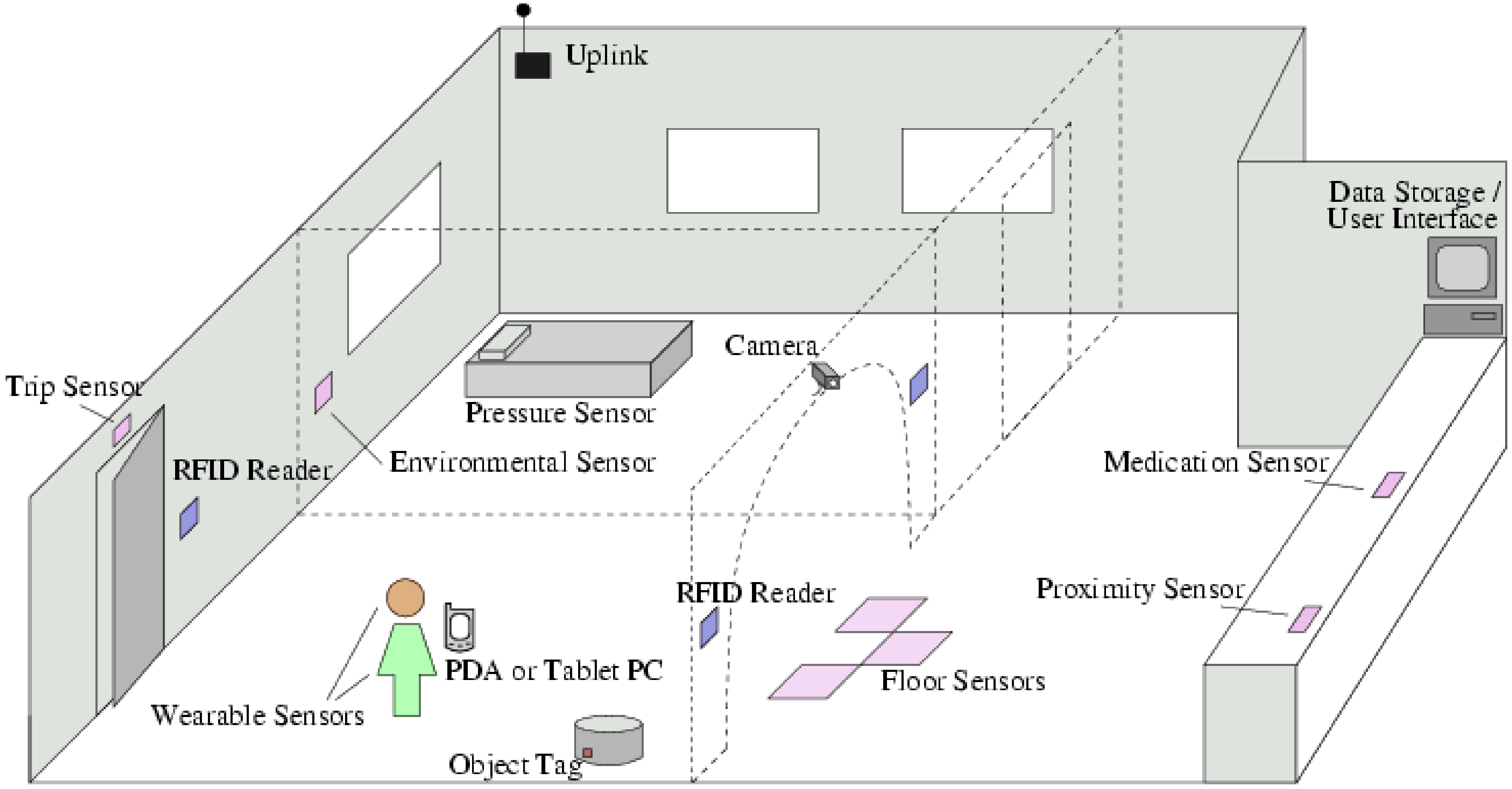
Challenge 1: Openness

- Typical closed systems design not applicable

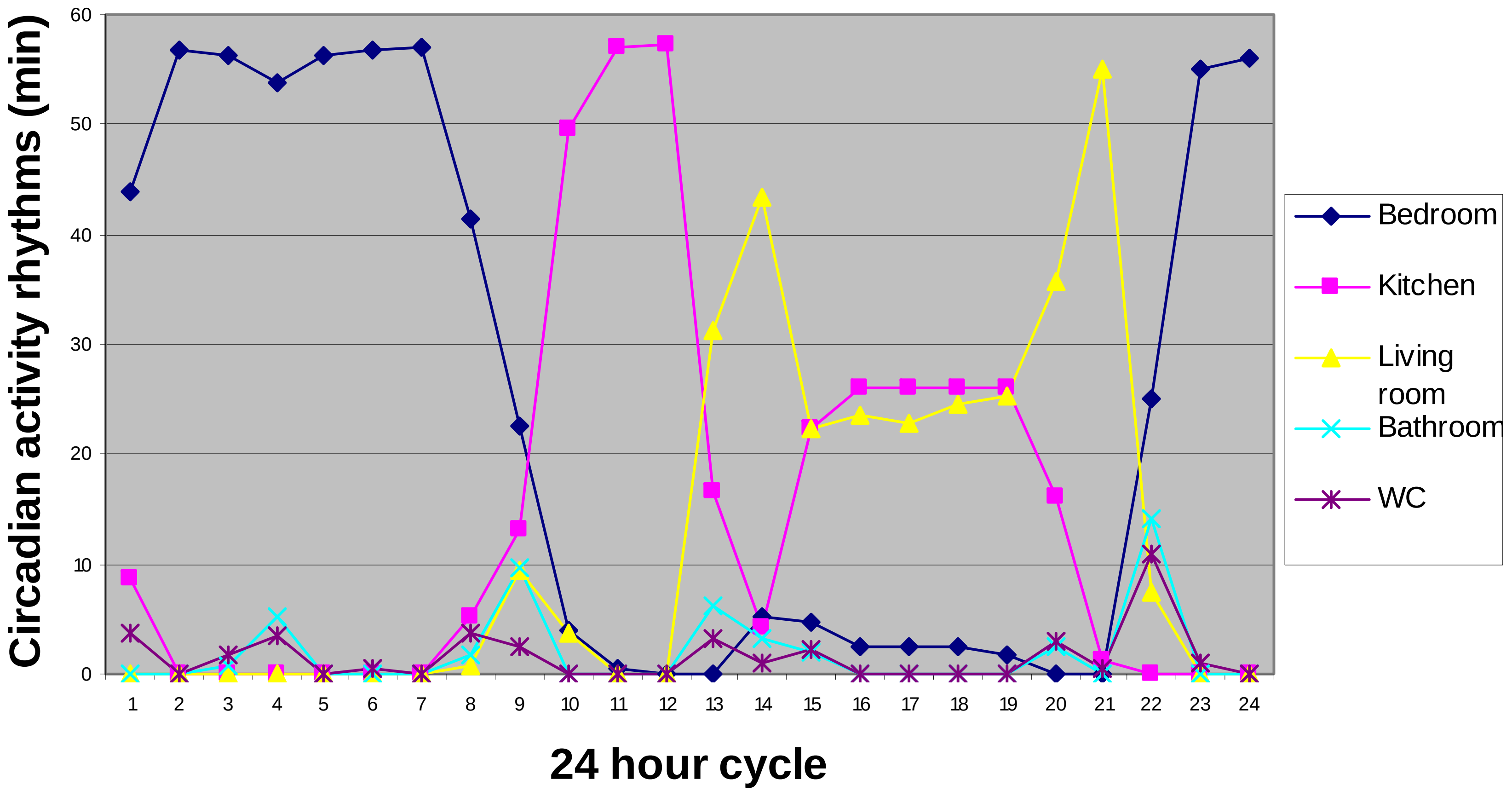
- Openness is a good thing
  - Systems interact with each other
  - Systems evolve over time
  - Physical environment itself changes

- High levels of uncertainty
  - Guarantees possible?

Smart Homes for Healthcare

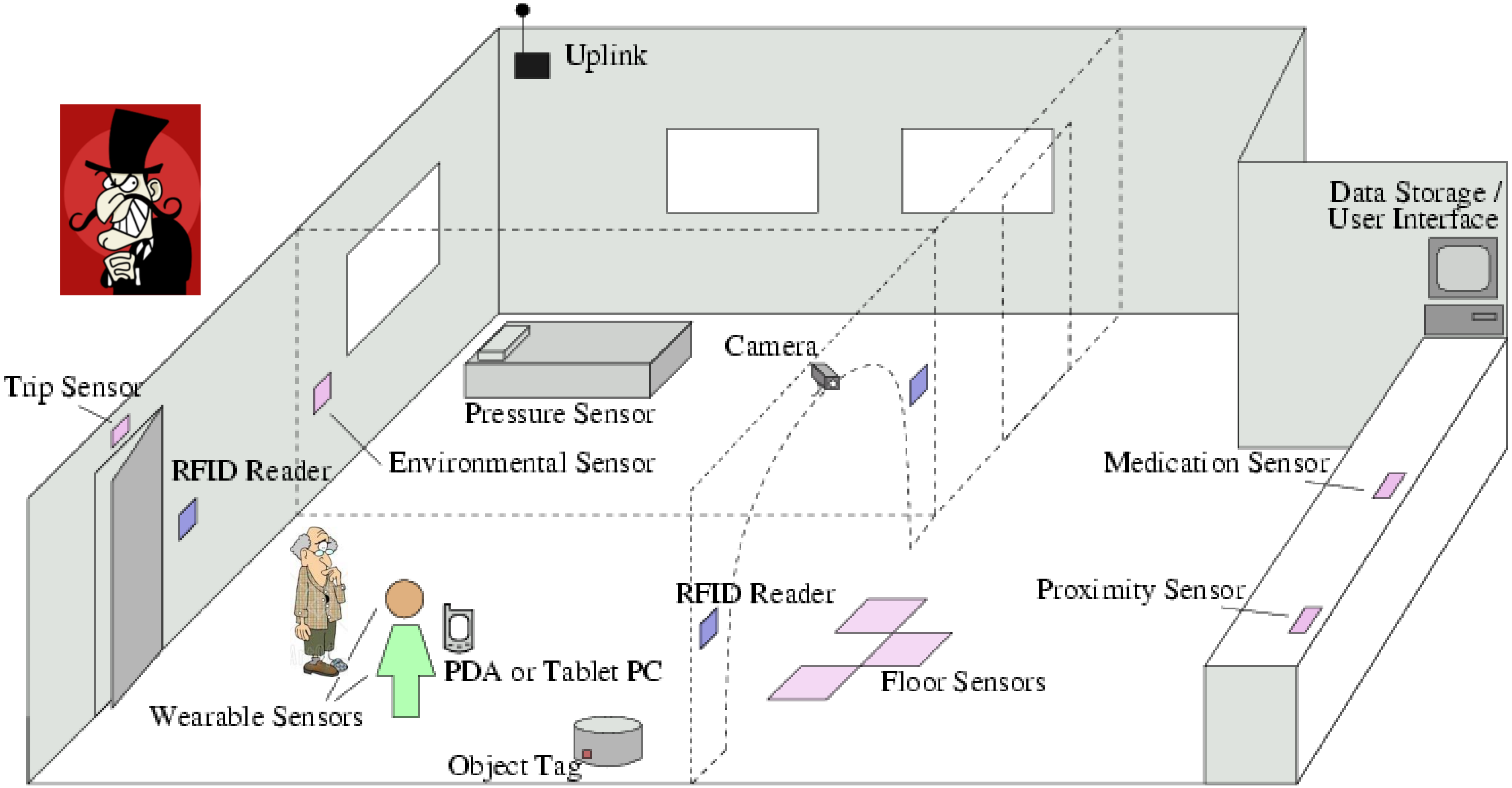


Circadian Rhythms



Circadian activity rhythm per room for 70 days

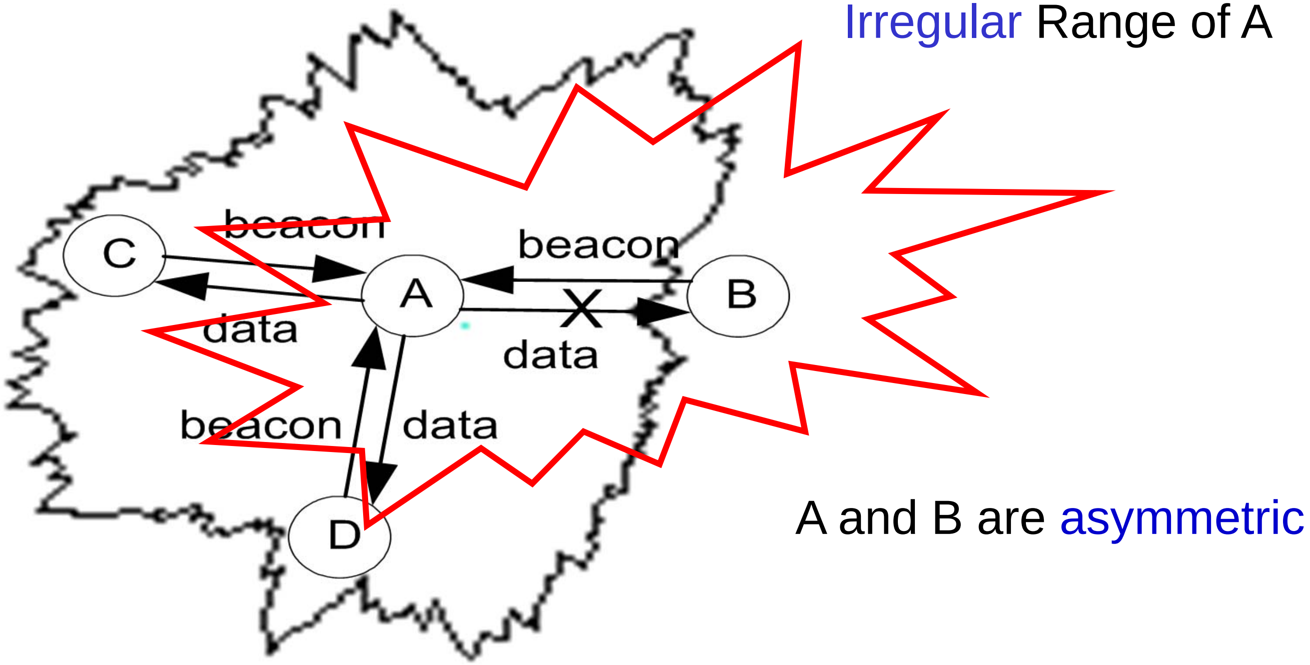
"Open" Smart Homes



Challenge 2: Environment

- How to model?
  - Methods to abstract the environment
  - Physical properties, weather, obstacles, temperature…
- How to identify all factors affecting the system?
- What does the correctness mean in an open system?
  - Formal methods have difficulty to address it
  - Validation-based approach
- The system design should consider the impact of the physical on the cyber

Example: Wireless Communication



Assume B, C, and D are the same distance from A.

Note that the pattern changes over time

Environment Abstraction

- Wireless communication
  - Interference
  - Burst packet losses
  - Fading
- Sensing and actuation
  - Target properties
  - Wake-up delays
  - Obstacles
  - Conflicting control loops
- External conditions
  - Weather
  - Temperature

Challenge 3: Robustness

- CPS should support operating in open and dynamic environments, with possible errors and failures
  - Correct execution of systems under specific assumptions is not enough
    - What if assumptions are not satisfied?
  - Complex physical properties of environments render "individual" solutions brittle
- How to model possible failures?
  - How to ensure all the important issues are covered
  - How to handle uncertainties and non-fail-stop failures
- How to validate that system satisfies correctness?

Approaches for Robustness

- How to validate that system satisfies correctness?
  - Validation using run-time assurance

Run-Time Assurance of Application-Level Requirements in Wireless Sensor Networks, ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN'10), Stockholm, Sweden, April 2010.

- How to design system to effectively deal with non-fail-stop failures?
  - Using failure severity and simultaneous classifiers

Being SMART About failures: Assessing Repairs in Smart Homes, 14th ACM International Conference on Ubiquitous Computing (Ubicomp'12), Pittsburgh, Pennsylvania, Sept. 2012.

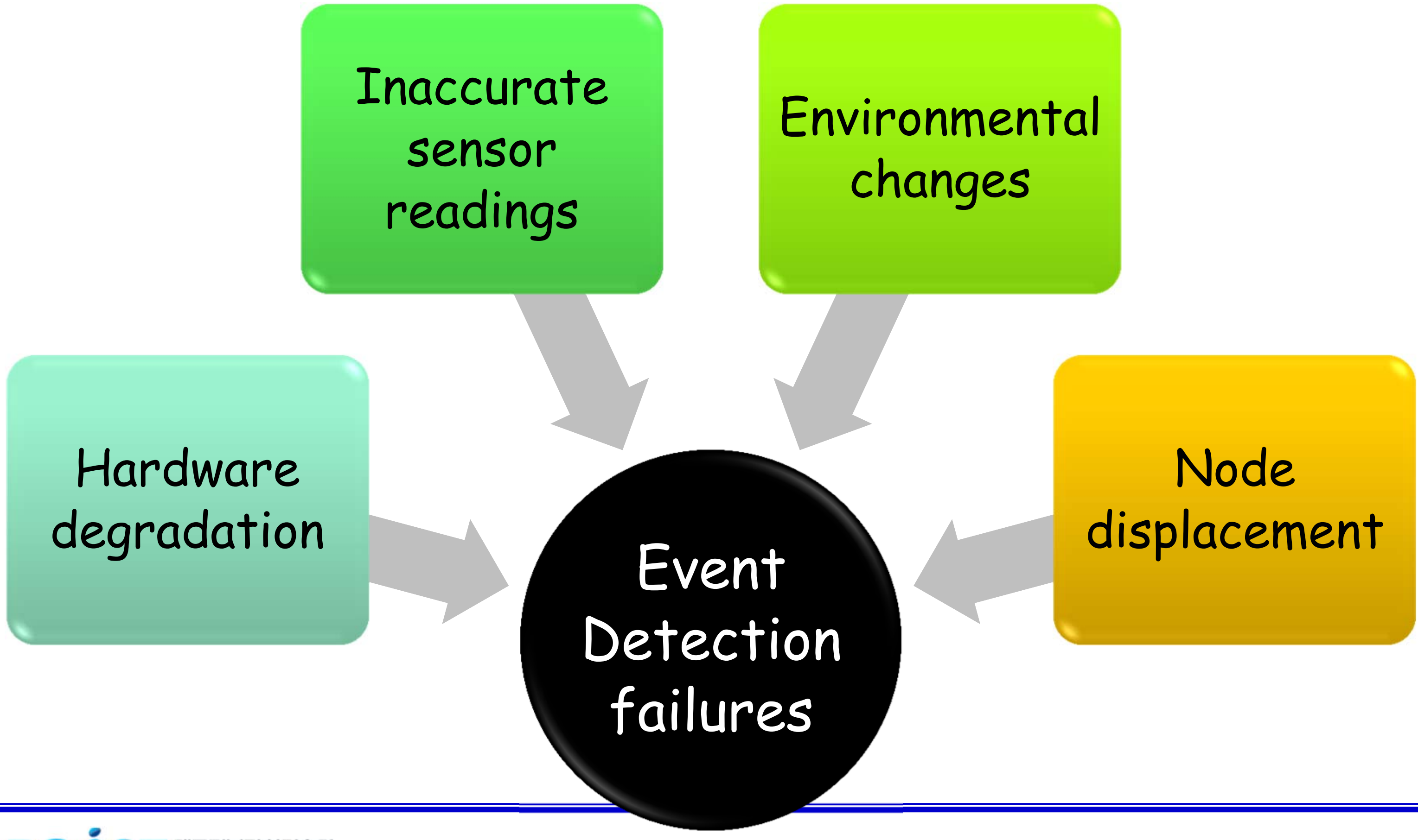
Validation using Run-Time Assurance

- Validate and re-validate that system is still operational
  - Formally specify application level semantics of correctness
  - Identify features that should be explicitly validated
  - Provide system configuration and key properties
  - Develop test specifications

- Combining them to provide a framework that offers ability to demonstrate that system is satisfying the correctness requirements at the semantic level, before problems occur

Dealing with Non-Fail-Stop Failures

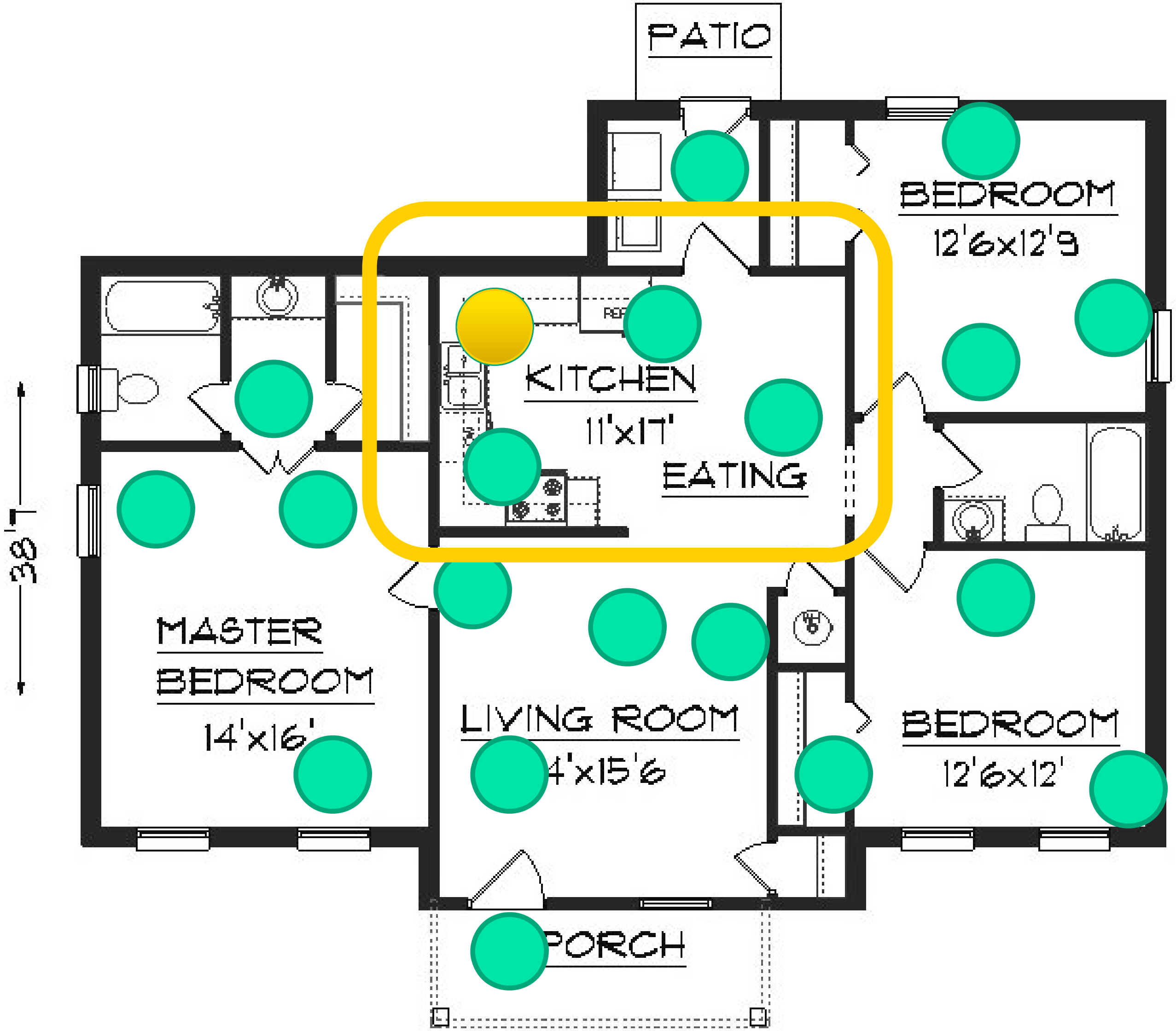
Continuous and robust event detection in CPS applications is extremely difficult to guarantee



Ideas

- Not all failures are equal
  - Assessing the severity of sensor failures
- Using a classifier ensemble where classifiers are preemptively trained for the occurrence of node failures
  - Detect non-fail-stop failures
  - Adapt the event detection to node failures and maintain sufficient application accuracy

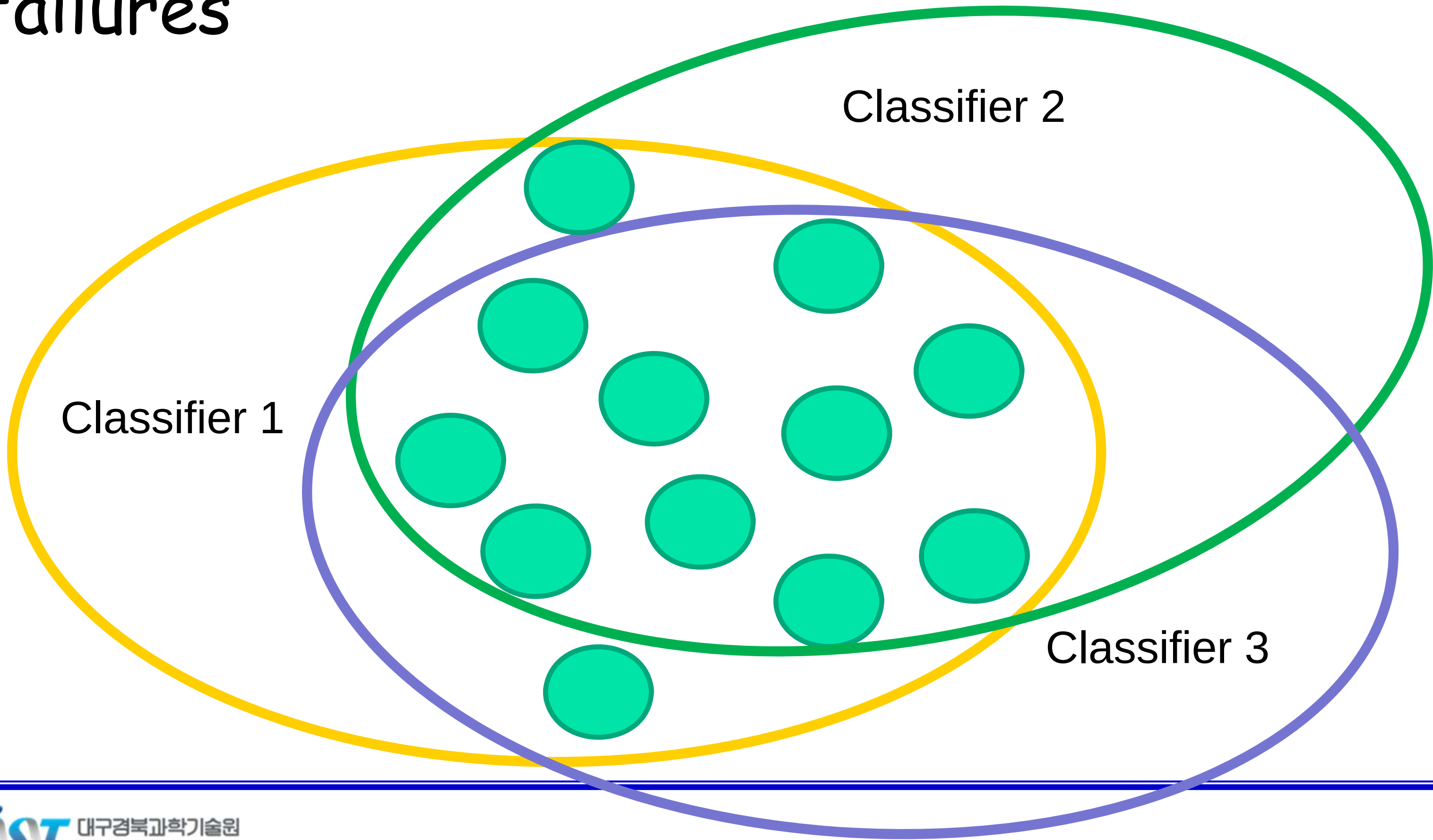
Failure Severity



31

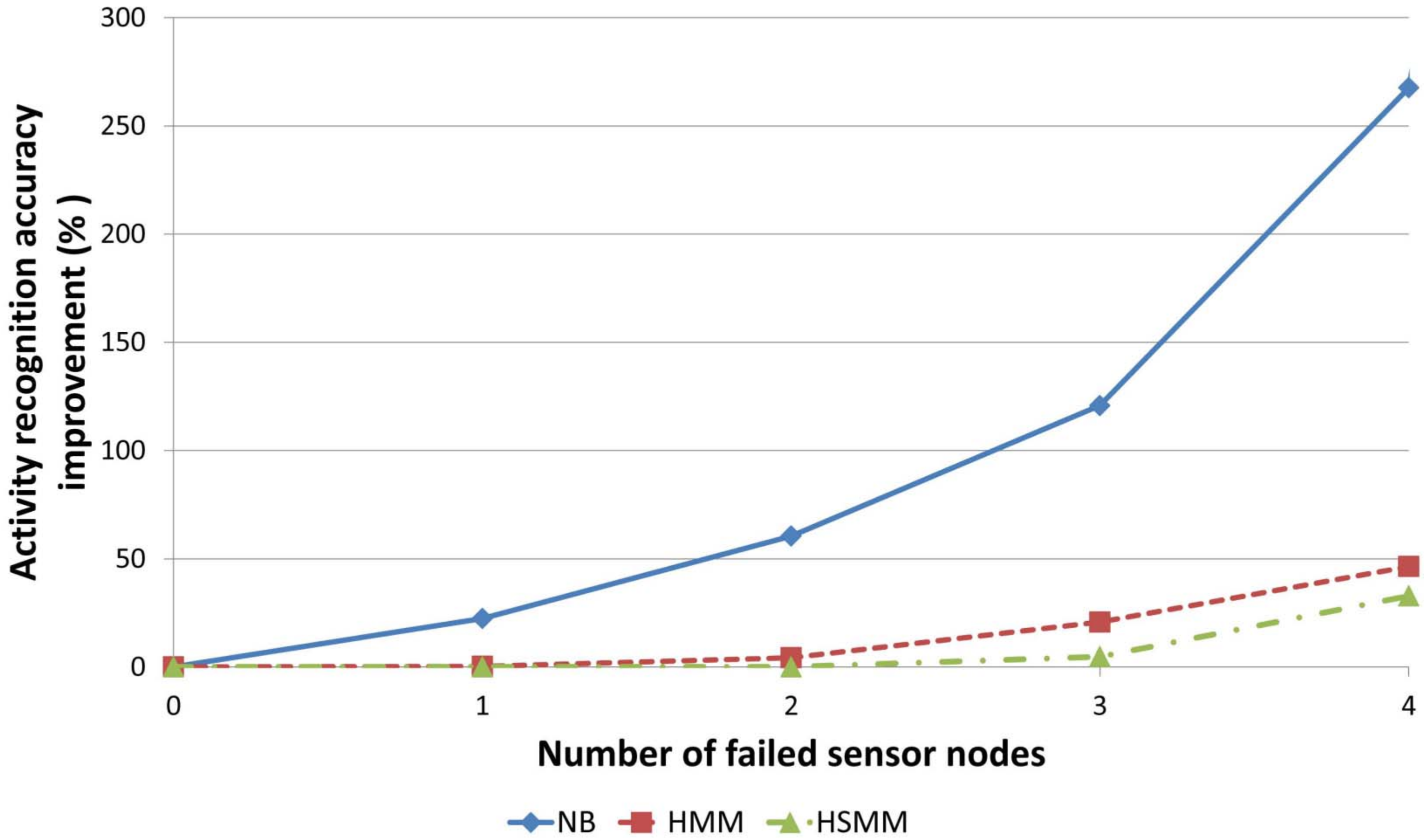
Multiple Classifiers

- If we preemptively assume that there will be failures, we can train classifiers for those failures



Detection Accuracy Improvement

Compared to NB, HMM, HSMM classifiers trained with all nodes in the system, SMART significantly improves the event detection accuracy in the presence of failures.



Institute of Science & Technology

Challenge 4: Security

- Will future CPS secure enough?
- Attacks
  - Physical objects and control loops
  - Need to identify vulnerabilities
- How to develop a system secure enough?

Examples of Attack

Researchers have managed to hack into vehicle computer systems and remotely take control of a car on the move

Examples of Attack

TECHNOLOGY | APRIL 8, 2009

Electricity Grid in U.S. Penetrated By Spies

Article | Video | Comments (146)

Email | Printer Friendly | Share: Yahoo Buzz | Text Size

By SIOBHAN GORMAN

Associated Press

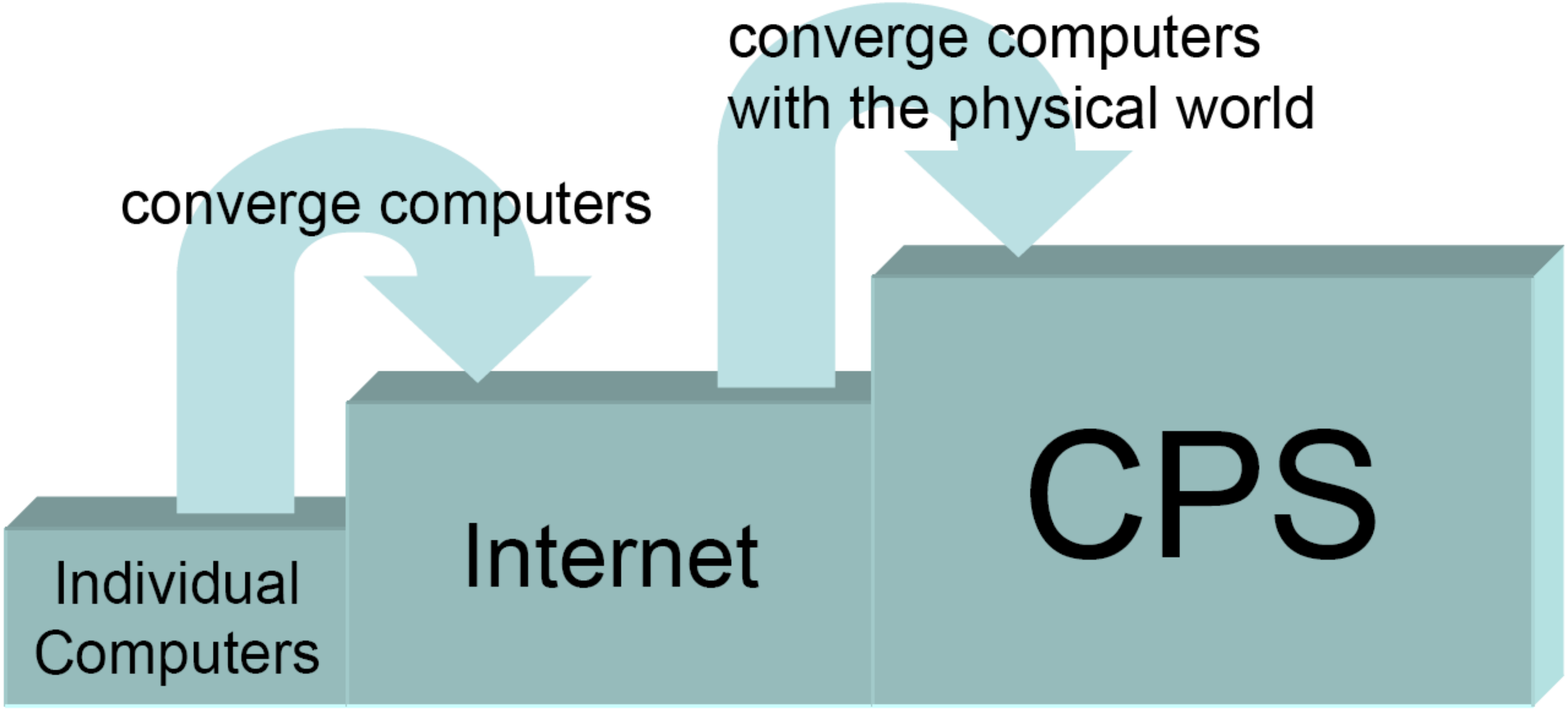
Robert Moran monitors an electric grid in Dallas. Such infrastructure grids across the country are vulnerable to cyberattacks.

WASHINGTON -- Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national-security officials.

Challenge 5: Real-Time

- Hard deadlines in CPS
- Hard deadlines associated with safety critical functions
- Mixed criticality systems in which the criticality levels demanded by tasks are diverse
- Time-based QoS
- Dynamically changing platform
- Designing systems to support hard real-time requirements in distributed dynamic environment is hard

Is CPS Next Big Thing?



Credit: Q. Wang

CPS Global Center @ DGIST

Research Collaboration Areas

CPS Fundamental Research

Medical CPS

- Medical devices & systems (Penn)
- Personalized health care (UVA)
- Safety using video/audio engines (UVA)

Energy CPS

- Smart Homes and Buildings (UVA)
  - Robust ADL detection
  - Energy management systems

Mobility CPS

- Smart Vehicles (CMU)
- Robustness in Extreme Conditions (Michigan)
- Human-centered Intelligent Transportation Systems (UVA)

Summary

- CPS: A number of sensor/actuator nodes to monitor and interact with physical environments/entities, enabling dramatic innovations in a variety of areas
- A large number of applications of CPS
  - Infrastructure monitoring
  - Surveillance and firefighting
  - Intelligent highways and automobiles
  - Smart buildings and power grids
- High degree of uncertainty
  - Point solution is not enough-> Robustness is a key
- We have just begun -- lots of research issues remain